

Úvod do informační bezpečnosti

PV080

Vašek Matyáš (část slajdů J. Bouda)

Bezpečnost (angl. *Security*)

Vlastnost prvku (např. IS), který je na určité úrovni chráněn proti ztrátám nebo také stav ochrany (na určité úrovni) proti ztrátám.

Bezpečnost

1. Prevence
2. Detekce
3. Reakce

Informační dominance

1. Cíl: Dosažení vlastní *informační dominance*, tzn. mít správné informace na správném místě ve správný čas.
2. Cíl: Zamezit nepřátelské straně v dosažení informační dominance.

Při utajení dat zvažujeme:

1. zda tato data mají být utajována,
2. zda samotná existence těchto dat je utajována,
3. zda i důvod utajení těchto dat je utajován.

Od aktiva k útoku

- **Aktiva** – data, zdroje... – s hodnotou
- **Zranitelnost** (systému) a útočník => **hrozba**
- **Riziko** – pravděpodobnost uplatnění hrozby
- **Útok** je realizací hrozby, útok může být **úspěšný** či **neúspěšný**
 - Úspěšný únik má dopad na hodnotu aktiv

Od rizika k bezpečnostní politice

- **Riziko omezujeme**
 - odstranění nemožné či příliš nákladné (častěji)
- **Bezpečnostní opatření** mají omezit rizika
- **Bezpečnostní mechanismy** implementují bezpečnostní opatření
- **Bezpečnostní politika** specifikuje způsoby uplatňování bezpečnostních opatření

Kde může selhat bezpečnost

- Matematický algoritmus
 - Velmi nepravděpodobné a neobvyklé
 - Může se stát jen při hrubé chybě výrobce systému
 - GSM
- Špatné naprogramování matematického algoritmu
 - Dost neobvyklé, stává se pouze u nekvalitních firem
 - Je důsledkem nedostatečného vzdělání programátorů
 - Nevhodný způsob generování náhodných čísel

Kde může selhat bezpečnost

- Chyby při implementaci systému
 - Velmi časté
 - Způsobeny snahou firem o minimalizaci nákladů při vývoji
 - Softwarové firmy nenesou odpovědnost za škody způsobené bezpečnostními chybami
 - Škoda na jejich pověsti není tak velká, aby se jim vyplatilo investovat peníze do kvalitního vývoje

Kde může selhat bezpečnost

- Všechny předchozí důvody zaviňují pouze ~ 5 % všech prolomení bezpečnosti!
- Hlavním důvodem prolomení jsou chyby a úmyslné jednání obsluhy počítačů
 - Snadno zapamatovatelné a tedy i uhodnutelné heslo
 - Použití nevhodných programů, které heslo neúmyslně zveřejňují – nezabezpečený přenos dat po Internetu

Incidenty způsobeny

- Chybami (neúmyslné): 50-70 %
- Vlivem přírody, zdrojů: 10-15 %
- Škodlivým softwarem: 5-10 %
- Záměrnými útoky (sabotáže) zaměstnanců (i bývalých) : 10-20 %
- Vnějšími útočníky: 1-5 %

Kde nejčastěji „selže“ bezpečnost

- Úmyslné jednání zaměstnanců
 - Pomsta zaměstnavateli nebo kolegům
 - Snaha obohatit se
 - Zaměstnanec je někým zkorumpován

Absolutně bezpečné systémy v praxi
NEEXISTUJÍ

Základní problém bezpečnosti

- Co útočník získá napadením daného systému?
- Kolik peněz, strojů, času a lidí musí nasadit na napadení daného systému?
- Vyplatí se to?
- Hromadné útoky na více systémů!

Klasifikace útočníků I

- Původní klasifikace 1-2-3, dnes nereprezentativní
- **Třída 0** (script kiddies) –útočníci, kteří nedisponují dostatkem znalostí o systému a využívají komukoliv běžně dostupné předpřipravené nástroje a postupy pro útoky na známé zranitelnosti – zkoušením těchto nástrojů metodou pokus-omyl nebo čistě náhodným necíleným zjištěním zranitelnosti (např. reakce zařízení na krátký a intenzivní výboj světla).
- **Třída 1** (chytří nezasvěcení útočníci) – mnohdy inteligentní útočníci, kteří nemají dostatek znalostí o systému. Využívají cenově běžně dostupných nástrojů nebo služeb s možností zmapování principu fungování přístroje v dohledné době. Obvykle zkouší útočit na známé bezpečnostní slabiny, nevyhledávají nové.

Klasifikace útočníků II

- **Třída 1.5** – jedná se o osoby nebo skupiny osob s možnostmi na rozhraní mezi 1. a 2. třídou. Útočníci jsou inteligentní, se základními znalostmi systému. Využívají cenově dostupných nástrojů, útočí na známé chyby a snaží se hledat i nové slabiny. Např. specializovaná pracoviště univerzit.
- **Třída 2** (zasvěcení insideři) – zkušení jedinci nebo týmy s nákladným a sofistikovaným vybavením, se kterým jsou schopni provést analýzu systému v dostatečném čase. Mají úzce specializované technické vědomosti a zkušenosti, různě hluboké pro jednotlivé části systému s možným přístupem k většině z nich.

Klasifikace útočníků III

- **Třída 3** (majetné organizace) – vysoce kvalifikované týmy využívající zařízení, která nejsou běžně dostupná na trhu. Mohou provádět detailní analýzy systému, navrhovat komplexní útoky a využívat nejmodernější analytické nástroje. Příkladem jsou např. vládní organizace (NSA), které mají pro své aktivity značné finanční zabezpečení.

Ochrana komunikace/dat

- Fyzická ochrana
 - místnosti
 - kabely
 - CD/DVD, USB tokeny
 - ...
- Kryptografie – umění (mj.) skrýt význam (informační hodnotu) dat
 - Návazná přednáška

Bezpečnost z dřívějšího pohledu

- **Důvěrnost:**

Cílem je zabránit zjištění sémantického obsahu dat nepovolanými (neautorizovanými) osobami.

- např. utajením existence informací (značně obtížné),
- kontrolou přístupu k místům, kde se data nacházejí,
- maskováním mezi jinými soubory nebo
- *změnou dat do jiné podoby, kterou nelze změnit zpět bez znalosti patřičné (tajné) informace – klíče. Tento poslední způsob se běžně označuje jako šifrování a budeme se mu věnovat dále v tomto kurzu.*

Bezpečnostní model Bell-LaPadula

- Procesy nesmějí číst data na vyšší úrovni (tzv. jednoduchá bezpečnostní vlastnost, též *NRU - no read up*).
- Procesy nesmějí zapisovat data do nižší úrovně (tzv. *-vlastnost, též *NWD - no write down*).

Bezpečnost z více úhlů pohledu

- **Integrita:**

*Data bez svolení majitele (autorizované osoby)
nesmí*

- nepozorovaně změnit svůj stav (tzv. slabá integrita)
 - nebo jej nesmí změnit vůbec (tzv. silná integrita).
- Pokud bude na dobré úrovni zajištěná důvěrnost, pak je zajištění integrity snazší.

Integritní model Biba

- Inverzní k modelu Bell-LaPadula
- Cílem je zajištění integrity dat
- Procesy nesmějí číst data na nižší úrovni – vlastnost *no read down*
- Procesy na dané úrovni nesmí zapsat data do vyšší úrovně – vlastnost *no write up*

Bezpečnost z více úhlů pohledu

- **Dostupnost:**

Autorizovaní uživatelé by měli mít přístup k datům a službám co nejméně komplikovaný.

– Dobře chráněná data, co se důvěrnosti a integrity týče, která nelze použít při řádné práci, ta nám nebudou příliš platná.

Bezpečnost z více úhlů pohledu

- **(Prokazatelná) Zodpovědnost:**

Za veškeré své činy a chování v systému mají uživatelé zodpovědnost vůči majiteli dat.

- Tato zodpovědnost nemusí být přímá (majitel nekontroluje každého uživatele osobně), ale v případě potřeby musí vždy existovat možnost zjistit, kde a kým (příp. i za jakým účelem) data v určitou dobu byla použita.

Bezpečnost z více úhlů pohledu

- Autentizace entit: *víme s kým komunikujeme.*
- Řízení přístupu: *přidělování dat/zdrojů kontrolováno.*
- Nepopiratelnost: *aktivitu nelze později popřít.*
 - Odeslání zprávy
 - Přijetí zprávy
- ...

Zásadní kroky pro zajištění bezpečnosti

1. Analýza a hodnocení hrozeb
2. Specifikace bezpečnostní politiky a architektury
3. Popis bezpečnostních mechanismů

Analýza a hodnocení hrozeb

- Zvážit, co všechno by mělo být chráněno
- Vyhodnotit, jaké hrozby hrozí ochraňovaným hodnotám.
 - Často nelze než vycházet z analýzy empirických poznatků o problémech v okolí, jiných útocích na podobné hodnoty atd.
- Chybně provedená analýza hrozeb má za důsledek téměř vždy chybně navržená bezpečnostní opatření. Hodnoty pak mohou být chráněny velmi nákladným, ale i naprosto nesmyslným a neúčinným způsobem.

Specifikace bezpečnostní politiky a architektury

- *Bezpečnostní politika* – co mají dosáhnout a zajistit ochranná opatření.
 - Zahrnuje požadavky, pravidla a postupy, určující způsob ochrany a zacházení s ochraňovanými hodnotami.
- *Architektura* na vysoké úrovni popisuje strukturu celého komplexu opatření a jednotlivým částem přiřadí bezpečnostní funkce.

Popis bezpečnostních mechanismů

- Zde jsou rozepsány techniky pro implementaci bezpečnostních funkcí nebo jejich částí.
- Účinnost mechanismu musí být v souladu s bezpečnostní politikou a přiměřená odpovídajícím hrozbám.

Nevhodnost doplňkové bezpečnosti

- Nejprve je pracně vybudován rozsáhlý systém a pak se přijde na to, že bude potřeba “nějak” zajistit ochranu spravovaných informací.
- Důsledkem pozdního doplnění specifikace o zajištění bezpečnosti může být
 - vybudování ochrany na nižší úrovni (než by za stejné peníze poskytla ochrana budovaná plánovitě)
 - nebo překročení rozpočtu,
 - mnohdy obojí.

Další oblasti bezpečnosti

- Prostředí
- Fyzická
- Personální
- Dokumentová (bez ohledu na formu)
- ...

Co je to bezpečnost ICT?

- Bezpečnost při používání systémů ICT obecně
 - Počítačová bezpečnost
 - Mobilní telefony
 - Kreditní karty
 - Internetové bankovníctví
 - ...
- Informační bezpečnost, kyberbezpečnost, počítačová bezpečnost... (rozdíly a překryvy)

Příklady zneužití

- Neoprávněné použití cizí kreditní karty
 - Výběr z bankomatu
 - Platba na terminálu (v obchodě)
 - Platba po Internetu (!)
- Zneužití mobilního telefonu
 - Odposlech telefonního hovoru
 - Volání na cizí účet
 - Zneužití falešné identity

Cíle bezpečnosti ICT

- Zamezit zneužití elektronických zařízení
- Nalézt osobu pokoušející se o zneužití
- Minimalizovat škody způsobené zneužitím
- ...

Více o praktických aspektech později v semestru...

Zajištění bezpečnosti

- jedná se o proces, nikoliv stav či cíl!
 - Výjimku by mohly tvořit systémy, které se samy vůbec nemění a kde beze změny je i jejich okolí. 😊

Autentizace entit (uživatelů)

Autentizace entit

- Elektronická zařízení musí navzájem prokazovat svou identitu
- Kreditní karta prokazuje svou identitu bankomatu
- Mobilní telefon (SIM karta) prokazuje svou identitu přijímající radiostanici mobilního operátora

Metody autentizace osob

- Znalost nějakého tajemství
 - PIN kreditní karty
 - Heslo pro telefonního bankéře
- Fyzická vlastnost (biometrika)
 - Otisk prstu
 - Sítnice oka
 - Hlas

Metody autentizace osob

- Vlastnictví nějakého předmětu (tokenu)
 - Vlastnictví kreditní karty
 - Vlastnictví SIM karty v mobilu
 - Vlastnictví klíče ke dveřím
- Kombinace předchozích
 - Kreditní karta a PIN
 - Občanský průkaz = token, fotka = biometrika

Metody autentizace

- SIM karta v mobilu je elektronické zařízení
- Moderní kreditní karty jsou elektronická zařízení
- Hlavním problémem autentizace je, aby se ten komu se prokazujete, nemohl později vydávat za vás
- Někdo může proces autentizace pozorovat, nahrávat, odposlouchávat

Metody autentizace

- Při vsunutí platební karty (s mag. proužkem) do bankomatu zloději použijí zařízení, které přečte magnetický pásek a umožní jim vytvořit kopii
- Nad bankomaty může být umístěna malá kamera, která nahraje zadávání PINu
- Zloděj takto získá kopii karty a PIN

Typy autentizace elektronických zařízení

- Pomocí hesla
 - Ověřující může ukrást identitu
- Pomocí důkazu nulového rozšíření znalostí
 - Osoba prokazuje, že zná řešení nějakého problému. Prokazování probíhá tak, že ověřovatel je na konci přesvědčen, že osoba dané tajemství zná, ale ověřovatel ani v budoucnu nebude schopen přesvědčit další osobu, že tajemství zná.

Mobilní telefony

Krádež mobilního telefonu

- Ukradený telefon lze i při zabezpečení PINem snadno odblokovat
- Najít člověka, který jej odblokuje je snadné a tedy i levné (stovky Kč u nelegálního odblokování PINu)
- Odblokování SIM karty je velmi nepravděpodobné
- Její používání po krádeži je nebezpečné

Krádež mobilního telefonu

- Mobilní telefon s ukradenou SIM kartou lze identifikovat, lokalizovat a následně zaměřit
- Zneužití údajů uložených v ukradeném telefonu
 - Telefonní seznam
 - Osobní plán
 - Záznamy o bankovních převodech
 - Audio, video, fotky, ...
 - Vydírání, krádeže, ...

Zneužití bezdrátového přenosu

- Odposlech telefonního hovoru
 - Šifrování v GSM má velmi nízkou bezpečnost
 - Do standardu byly (úmyslně?) zavedeny chyby, které měly zmást konkurenční telefonní společnosti.
 - V mnoha zemích (USA, Turecko, ...) se šifrování nepoužívá vůbec.
 - Lze odposlechnout díky jednoduchému zařízení.



Zneužití bezdrátového přenosu

- Volání „na cizí účet“
- Klasický odposlech
- Zneužití identity volaného
 - Poškození pověsti
 - Získání obchodních výhod
- Přes relativní snadnost vyžadují tyto útoky jisté technické znalosti
- Přejechod na standard 3GSM – navržen kvalitně

Zneužití přídatných zařízení

- Bluetooth
 - Handsfree, synchronizace s počítačem a PocketPC
 - Návrh obsahuje mnoho bezpečnostních chyb
 - Zařízení v mobilech mají udávaný dosah 10m
 - Bluetooth puška dokáže odposlech na 1 km



Zneužití operátorem

- Operátor může sledovat všechny hovory
 - Někteří zaměstnanci operátora mohou být schopni sledovat všechny hovory
- Záznam zvuku je zatím naštěstí relativně náročný na kapacitu úložných zařízení a obtížně se automatizuje jeho zpracování.
- SMS zprávy zaberou málo místa a snadno se automaticky vyhodnocují.

Zneužití operátorem

- SMS posílané z mobilu na mobil nebo z internetu při udání čísla odesilatele mohou být a někdy také jsou ukládány!
- Mohou být poskytnuty legálně na základě žádosti soudu, nebo nelegálně zneužity zaměstnancem – prodány třetí osobě.
- Je možné sledovat polohu mobilních telefonů!
- Data retention!!!

Polosemestrálka: 13.11.

Polosemestrální písemka – 30 bodů

- Do 11.11. – **nutná registrace** do skupin!
- Doba pro práci – 20 minut
 - I. skupina 8:00
 - II. skupina 8:33
 - III. skupina 9:09
- Příchod vždy spodním vchodem (řazení dle abecedy!!!), odchod horním vchodem.
- S sebou jen pero (2) a ISIC (nebo jiný doklad s aktuální fotografií a jménem).

Povinnosti správce osobních údajů:

- :c1 ověřovat neautorizované výskyty osob
- :c2 stanovit prostředky a způsob zpracování osobních údajů
- :c3 zpracovávat pouze pravdivé a přesné osobní údaje
- :c4 neposkytovat data třetím stranám před sepsáním Smlouvy o autorizovaném poskytnutí osobních dat
- :c5 archivovat data kódovaně, není-li řečeno jinak
- :c6 vkládat falešné záznamy, aby v případě krádeže dat nebylo možné snadno posoudit jejich validitu

:c1 -2

:c2 ok 3

:c3 ok 3

:c4 -1

:c5 -1

:c6 -1

Mezi základní pravidla bezpečnostního modelu Bell-LaPadula patří:

:c1 Procesy nesmějí číst data na vyšší úrovni.

:c2 Procesy nesmějí zapisovat data do vyšší úrovně.

:c3 Procesy nesmějí číst/zapisovat data z/do nižší úrovně.

:c4 Procesy nesmějí číst data na nižší úrovni.

:c5 Procesy nesmějí zapisovat data do nižší úrovně.

:c1 ok 2

:c2 -2

:c3 -2

:c4 -2

:c5 ok 2